How Higher–Performance PCs Can Enhance Information Security

Essential
Business
Technologies
Series

Performance with Purpose

Got a minute?

When it comes to information technology, one thing's for sure — the pace of innovation shows no signs of slowing.

That's good, because if your company applies the latest technologies faster and more effectively than your competition, you can gain a significant edge.

But first, you have to learn what each new application or technology is all about.

It's not easy. Who has time to sort through the wealth of material and find the nuggets of relevant information? Who wants to wade through the hype to find the substance?

This series is designed to help. Each booklet provides a quick, no-spin overview of an essential new business technology — what it is, how it can benefit your company and how it's likely to impact your enterprise infrastructure.

When you're done reading, you should have a better understanding of a key enabler of next-generation computing — and maybe even saved a few minutes along the way.

Worried?

Intel co-founder and chairman Andrew S. Grove wasn't thinking of information security when he titled his 1996 bestseller, "Only the Paranoid Survive." Grove was referring to the dangers successful corporations face when they become complacent. Rest on your laurels and a leaner, hungrier competitor will swoop in with products that are faster, cheaper or more innovative. A touch of paranoia, Grove argued, can help your company avoid complacence and fend off competitive threats.

But his motto fits today's security scene remarkably well. As recent, widely publicized security breaches make clear, there's a dangerous world of pranksters, thieves and disgruntled employees determined to use information technology to steal valuable data, disrupt business and embarrass corporations. And the havoc these cyber criminals can wreak is growing as companies store more information on the network, conduct rising numbers of transactions online, and bring collaborative partners into a broader array of electronic business processes.

A degree of paranoia about the hazards of our interconnected computing universe is both realistic and protective. No one wants a locked-down environment with onerous policies that limit agility and productivity. But you also can't afford to be complacent about security.

IT managers have gotten the message. Gartner Group, the industry analyst firm, says IT managers ranked security and privacy their second highest IT spending priority for 2002[1]. International Data Corp (IDC) predicts worldwide spending on Internet security software will reach $14 billion in 2005.[2]

Cyber crime knows no national boundaries. A recent report from the Australian Institute of Criminology says up to 10 percent of online consumer transactions in Asia involve some type of fraud, with similar rates likely for business and government transactions. The value for these fraudulent transactions could be as high as U.S. $91 billion.[3]

Organizations that track security breaches say enterprise attacks are rising sharply. The CERT* Coordination Center reports 52,658 incidents in 2001, up nearly 250 percent from the 21,756 in 2000 — and each incident may affect one site or thousands.[4]

The Computer Security Institute (CSI), working with the San Francisco FBI's Computer Intrusion Squad, surveys computer security specialists working in U.S. corporations, government agencies, financial and medical institutions, and universities. Their 2001 survey of 538 practitioners found 85 percent had detected computer security breaches in the previous 12 months and 64 percent experienced financial losses from them. Those that quantified their financial losses pegged them at $377.8M — a significant increase from 2000, when 249 respondents reported losses totaling $92.9M.[5]

Where are the risks?

Not to put too fine a point on it: everywhere. Information security vulnerabilities occur throughout the enterprise. Any networked resource can be attacked over the LAN or Internet. Networks can experience denial of service attacks. Applications can be corrupted and information stolen from servers and clients. Hackers can trick you into sharing intellectual property by hiding behind collaboration technologies. Data can be swiped even from non-networked systems.

Whether attackers want to commit information theft and fraud, disrupt your business operations or simply prove a point, they have many ways to do damage:

- Destroying files and applications via a virus, trojan horse, worm or other malicious code.
- Gaining access to your systems and network by cracking or stealing passwords, eavesdropping electronically, or manipulating networking protocols.
- Shutting down your Web site through a denial of service attack.
- Impersonating a trusted system (spoofing) or a user (e-mail hacking or identify theft).

What's the solution?

You don't expect one approach to protect all your physical assets. Instead, you lock the doors and windows, get a burglar alarm system, install perimeter lighting, and hire security guards.

It's the same with information security. No technology or policy does everything, and none is foolproof. So, you need a multi-layer architecture with overlapping technologies to protect every aspect of your information environment. Here are the most widely used solutions:

- Firewalls. The front line of defense for many companies, firewalls sit between the corporate intranet and the Internet, and manage public access to the network's resources and data. They can also be used within the enterprise to provide an additional layer of security for your most sensitive systems.
- Intrusion detection. If firewalls are the lock on the front door, intrusion detection systems (IDS) are the burglar alarm system. IDS can monitor host or network activity to trigger an alert or take action if they detect an attempted or successful intrusion.
- Virus protection. Viruses are self-replicating, malicious programs, often carried in email attachments, that can spread rapidly across a network, deleting and modifying files and causing other damage. Both email servers and client systems need virus protection.
- Authentication & authorization. Modern, network-based business rests on a foundation of trust. Authentication and authorization technologies help ensure that the people and systems you do business with are who they say they are.
- Encryption. From marketing plans stored on a user's hard drive to contracts sent through email, encryption can increase the integrity of sensitive data and offer greater levels of protection from prying eyes.

"You need to protect every single door, window and crawlspace."

Charles Kolodgy
Research manager for Internet Security, International Data Corp. (IDC)

Areas of Vulnerability

Any resource on the network is vulnerable to attack.

Internet & Intranet

Network

- Denial of service
- Data integrity
- Spoofing
- Replay
- Snooping

Server

- Denial of service
- Data theft from HD
- Data integrity
- Change in server administration and superusers

Client

- Data theft and integrity
- Malicious code (e.g. viruses, macros, etc.)
- Access to corporate network

Technologies for a Solution

A comprehensive solution depends on multiple technologies to protect clients, servers and networks.

Internet & Intranet

Network

- Firewall
- IPSec
- VPNs
- SSL & TLS

Server

- Access control and policy management
- Firewall
- Encryption
- Digital signature
- Multi-factor authentication
- Trusted key storage

Client

- Encryption
- Digital signatures
- Access control/policy
- Protected execution
- Trusted key storage
- Digital watermark
- Metering
- ATA disk lock
- IPSec
- Smart cards
- Biometrics

How do information security technologies impact my enterprise infrastructure?

Because virtually any element of the distributed, networked infrastructure is susceptible to hacking, solutions must encompass every element of the computing infrastructure. That means servers, clients, and networks will all be affected by the performance and bandwidth impacts of security technologies.

For example, servers and clients need enough horsepower to handle demanding tasks such as encryption and authentication without slowing system responsiveness. Servers and appliances that run solutions such as firewalls or intrusion detection systems must be powerful enough to accommodate surges in traffic.

If any of these systems lack the requisite performance, user productivity and organizational effectiveness can suffer. For client systems this is especially true, since people will often avoid using features that cause an unacceptable performance hit. When that happens, organizations not only lose the value of their security investments, but also put their information security at risk.

Planning your information security strategy?

Be proactive. Don't wait for a serious breach before you take action.

Start with policies. Policies are the cornerstone of a secure enterprise. Put them in place and educate your staff so everyone makes security a priority.

Decide how much security you need and can afford. Not every asset warrants the same level of protection. Decide how much risk you can accept and proceed accordingly.

Plan for the worst. Develop an incident response team and determine how to respond to an attack.

Keep current. Install the latest patches and signature files to keep your technologies up to date.

Remember the human element. Simple changes like enforcing strong passwords can deliver a big payoff.

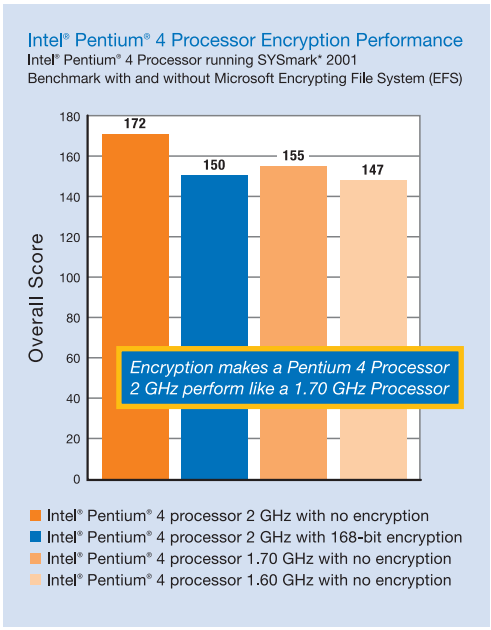
How can PCs based on the Intel® Pentium® 4 processor make a difference?

Client systems play an important role in enterprise information security. To maximize security, client systems should run a variety of information security technologies:

- Anti-virus software with continuous scanning, so the system is safeguarded against viruses lurking in e-mail attachments, web downloads, or even screen savers.
- Encryption, to protect files stored on the hard drive and sensitive information sent as email attachments.
- Public key cryptography, such as the Public Key Infrastructure (PKI), are essential services for providing strong authentication, access control and data integrity.
- Personal firewalls protect client systems from attacks while also limiting users' ability to gain unauthorized access to network resources.

These technologies often run transparently in the background, adding to the demands on the system while the user is trying to get work done. And they can consume enough processing cycles to have a noticeable impact on the system's responsiveness. Industry-standard benchmarks show that when a PC powered by an Intel® Pentium® 4 processor at 2 GHz ran the BAPCo* SYSmark2001* benchmark with the Microsoft* Encrypting File System's 168-bit encryption activated, its performance on common productivity tasks slowed enough to put it at about the same level as a Pentium 4 processor at 1.70 GHz. So, any company purchasing client systems will want to secure enough headroom to accommodate the demands of security tasks and maintain responsiveness for the user.

PCs based on the Pentium 4 processor also provide an outstanding platform for a wide range of security appliances and management consoles. With their clock speeds of 2.40 GHz and rising, and innovative Intel® NetBurst® microarchitecture, Pentium 4 processors offer performance with purpose, for superb responsiveness on demanding security tasks.



The calculations required for 168-bit encryption slowed the Intel® Pentium® 4 processor 2 GHz's performance on typical office productivity tasks down to about the same level as a Pentium 4 processor 1.70 GHz without encryption.

Configuration Details. Source: Intel. Configuration: Intel® Pentium® 4 processor - Intel® Desktop Board D850MD, 256MB PC800 RDRAM -45; Intel® 850 chipset platform; IBM* 30GB ATA-100 DTLA-307030 hard drive, Intel® chipset INF file v3.200.1008, Intel® Application Accelerator Storage Driver v1.01, Leadtek* WinFast/ nVidia* GeForce*3 4x AGP, nVidia Detonator* 4 v21.81 graphics driver, 1024x768 at 16-bit color, DirectX* 8.1, Windows* XP, 100 Mbps LAN; Intel® C & Fortran compilers 5.01 for SPEC; Intel® Pro/100+ PCI LAN.

Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of Intel products as measured by tz hose tests. Any difference in system hardware or software design or configuration may affect actual performance.

Security technologies are becoming more pervasive. Case in point: Microsoft* Windows XP* and Windows .NET* Server provide a range of security features, including PKI enhancements; authentication options such as smart cards, Kerberos and X.509 certifications; and strong encryption services such as IPSec. The Microsoft Encrypting File System (EFS) is standard with Windows* 2000 and Windows XP, so organizations can easily encrypt and protect the files on the client's hard drive. Windows XP Professional also supports stronger Federal Information Processing Standards (FIPS) 140-1 compliant encryption algorithms such as 3DES.

Cyber Security: Cost and Impact[6]

Action	Cost	Security Impact
Dedicate one staff member to maintaining security systems.	$	****
Educate staff and promote awareness.	$	****
Schedule regular virus and patch upgrades, firewall reconfiguration, PC security audits, etc.	$$	***
Hire or reassign staff to create and enforce security policies.	$$	***
Install basic hardware and software: firewalls, antivirus software, passwords, etc.	$$$	**
Buy advanced hardware and software, such as encryption, token authentication, digital certificates and signatures.	$$$	***
Outsource your worries.	$$$$	****
Hire or train programmers to write security code.	$$$$	***
Conduct regular security and penetration audits or assessments.	$$$$	***

Information Security ROI

Need hard data to justify your security spending? Researchers are turning up quantifiable evidence of the return on security investments (ROSI).[7]

A team from MIT, Stanford and @Stake, a Massachusetts-based security consulting firm, has demonstrated that the earlier developers code security into their software, the higher the ROI. Building security into the design stage nets a 21 percent ROSI.

A company that expects to lose $100,000 annually due to network intrusions will experience a ROSI of $45,000 if it purchases a $40,000 IDS system that's 85 percent effective, according to a formula developed by researchers at the University of Idaho.

Carnegie Mellon has shown that higher information security spending helps minimize the damage from an attack.

What's next?

The information security goal won't change — companies will continue to need to protect corporate resources and ensure the integrity of their business transactions. But many factors will raise the stakes and make security technologies even more pervasive and essential.

The expansion of collaboration and the rising volume of business transactions over the Web will make trust more important than ever. Organizations will place a greater emphasis on robust authentication and authorization and strong encryption, and will use PKI and other authentication technologies to help create a secure and trusted communications infrastructure. Clients and servers alike will be expected to prove they're who they say they are and can be trusted, i.e., don't have malicious code.

Web services depend on the ability to validate the integrity of the code being downloaded, so code signing with digital certificates will become the norm.

Wireless networks will take on more robust encryption and protocols to foil electronic eavesdroppers.

Emerging technologies such as biometric identification will offer new opportunities to ensure secure access to confidential resources.

Above all, companies will become more deeply aware that information security must be an integrated management discipline, not a piecemeal solution.

Terms and Acronyms

Authentication	The use of technologies such as smart cards, kerberos, and PKI to identify an entity such as a user, system, or application.
Digital certificate	Electronic files that uniquely identify people and resources over a network.
DoS	Denial of service. An attack that attempts to shut down a system or service by flooding it with more requests than it can handle.
IDS	Intrusion detection system. Host- or network-based software or appliances that search for evidence of an intrusion and notify an administrator or take action to stop it.
IPsec	Internet Protocol Security. A core technology for virtual private networks, IPsec is a set of protocols that supports the secure exchange of packets at the Internet Protocol (IP) layer.
PKI	Public Key Infrastructure. Technology for managing digital certificates and encryption keys.
Spoofing	Pretending to be another system or individual.
TCPA	Trusted Computing Platform Alliance. An industry working group established in 1999 by Compaq, HP, IBM, Intel and Microsoft and now encompassing over 135 companies devoted to enhancing the integrity, authenticity and privacy of Internet-based communications and commerce.

[1] Smart Business Magazine (www.smartbusinessmag.com), Dec. 01-Jan. 02 edition.

[2] InfoWorld, IDC: Security Software to Total Billions by 2004.
www.infoworld.com/articles/hn/xml/01/04/18/010418hnsecuritymarket.xml

[3] CNN.com, Fraud Hits One in Ten Asian Internet Deals, March 20, 2002.
http://www.cnn.com/2002/BUSINESS/asia/03/20/asia.net/index.html

[4] http://www.cert.org/stats/cert_stats.html.

[5] CSI, Financial Losses Due to Internet Intrusions, Trade Secret Theft and Other Cyber Crimes Soar, 2001.
http://www.gocsi.com/prelea/00321.html

[6] Adapted from CIO Magazine, How to Plan for the Inevitable, March 15, 2002.
http://www.cio.com/archive/031502/plan_sidebar1_content.html

[7] CIO Magazine, Finally, a Real Return on Security Spending, Feb. 15, 2002.
http://www.cio.com/archive/021502/security_content.html

[8] For more information, see: http://www.intel.com/ebusiness/products/itanium/overview/bm012101.htm
http://www.intel.com/ebusiness/products/server/processor/xeon_mp/bm021101.htm

[9] For more information, see: http://www.intel.com/network/idc/products/ecommerce_equipment.htm

Intel and Information Security

Intel is well known as the company whose state-of-the-art microprocessors are “inside” the world’s leading personal and laptop computers. In addition, Intel provides an array of building block technologies for the Internet economy, from servers to network components to hand-held wireless devices.

Intel incorporates industry-leading security technologies into many of these building blocks. For example, servers based on the Intel® Itanium™ and Xeon™ processors offer outstanding performance and price-performance for e-Commerce transactions.[8] Intel® NetStructure™ 7800 series e-Commerce accelerators provide patent-pending technology that boosts SSL transaction performance and enhances data center efficiency by offloading cryptographic functions from the server.[9]

Intel also works with other companies and institutions to develop industry standards that address security challenges.

Performance with Purpose

Learn more about information security solutions — and how Intel® Pentium® 4 processor-based PCs can enhance them.

Pentium 4 Processors for Business
http://www.intel.com/ebusiness/products/desktop/p4p/index.htm

To order Securing Business Information: Strategies to Protect the Enterprise and Its Network by F. Christian Byrnes and Dale Kutnick, published by Intel press:
http://www.intel.com/intelpress/sum_book5.htm

Trusted Computing Platform Alliance
http://www.trustedpc.org

Computer Security Resource Center (sponsored by the U.S. National Institute of Standards and Technology's Computer Security Division)
http://csrc.nist.gov

CERT* Coordination Center at Carnegie Mellon University
http://www.sei.cmu.edu/about/press/CERT_press.html#links

Watch www.intel.com/info/pentium4 for other booklets in Intel's series of quick guides to essential business technologies:

- Collaboration
- e-Learning
- Information management
- Office productivity
- Web services
- XML

Printed in the USA/0502/ID/MP/10K 250951-001